

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

The premises at 1101 E Forest Hill Avenue, Oak Creek,
Wisconsin; and a 2008 black GMC Acadia bearing VIN#
1GKER13748J138676 and Wisconsin license plate 671NGF.

Case No. 20m 860

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 241

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



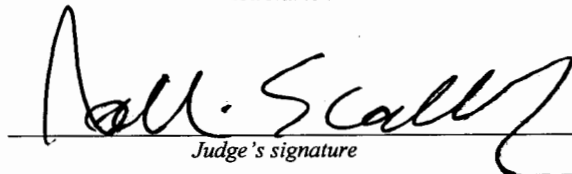
Applicant's signature

Special Agent Jessica Krueger

Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 14, 2020



Judge's signature

City and State: Milwaukee, Wisconsin

William E. Callahan

U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jessica Krueger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1101 E Forest Hill Avenue, Oak Creek, Wisconsin (hereinafter "Subject Premises"), and the vehicle identified as 2008 GMC Acadia bearing VIN# 1GKER13748J138676 (hereinafter referred to as "Subject Vehicle"), all further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the FBI and have been since November 2009. I am involved in investigations of persons suspected of violations of Federal law in the State of Wisconsin and throughout the United States. I have gained experience conducting investigations through formal training and consultation with local, state, and federal law enforcement agencies as well as from law enforcement investigations themselves. I have assisted in multiple criminal investigations and participated in numerous search and arrest warrants related to such investigations

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. The FBI is investigating criminal activity by members of an organization called "The Base," a neo-Nazi group that aims to unify militant white supremacists around the globe and provide them with paramilitary training in preparation for a "race war." As described herein, Yousef Omar Barasneh is a member of "The Base," and in September 2019, he conspired with others and participated in vandalizing a synagogue in Racine, Wisconsin, in violation of, among other things, and 18 U.S.C. § 241, which makes it a felony to "conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States." Relatedly, 42 U.S.C. § 1982, secures the right of all U.S. citizens to hold and use real and personal property, including property used for religious purposes.

5. On September 22, 2019, law enforcement officers in Wisconsin discovered that the Beth Israeli Sinai Congregation located at 3009 Washington

Avenue Racine, Wisconsin, had been vandalized. Specifically, the officers saw swastikas, the symbol for The Base, and anti-Semitic words spray-painted on the exterior of the building. The synagogue is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

6. Similarly, on September 21, 2019, law enforcement officers in Hancock, Michigan, discovered that the Temple Jacob had been vandalized. Specifically, they saw swastikas and the symbol of The Base spray-painted on the exterior of the building. As with the synagogue in Racine, Wisconsin, the synagogue in Michigan is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

7. Based on my training and experience and familiarity with this investigation, I am aware that The Base is a white, racially-motivated extremist group that describes itself as an “international survivalism & self-defense network, for nationalists of European descent,” and offers “IRL” (in real life) survivalist training to resist “our People's extinction,” or the extinction of the white race. Members of The Base communicate with each other through online platforms and encrypted online messaging applications and chat rooms. In these communications, they have discussed, among other things, acts of violence against minorities (including African Americans and Jewish-Americans), Base military training

camps, and ways to make improvised explosive devices ("IEDs"). The symbol used by The Base is a black flag with three white Runic Eihwaz symbols.

8. Based on information I have received during the course of this investigation, I am aware that The Base has been active in Wisconsin and that there are members of the "North Central region," alternatively known as the "Great Lakes cell," based in Wisconsin. For instance, in early June 2019, Base recruitment flyers were posted at Marquette University in Milwaukee, WI. In July 2019, The Base organized an armed training session for members in Wood County, Wisconsin, and posted photos to social media about the session. And, as noted above, the symbol for The Base was discovered spray-painted on the Beth Israel Sinai Congregation synagogue in Racine, WI.

9. As part of the investigation, the FBI received information from an individual associated with The Base, who I will refer to as co-conspirator #1 ("CC1"). In statements to the FBI between October 2019 and December 2019, CC1 admitted that in September 2019, he directed other members of The Base to vandalize minority-owned properties throughout the country. CC1 called this "Operation Kristallnacht"¹ and directed others to "tag the shit" out of synagogues. Based on my

¹ Based on publicly available information, I am aware that Operation Kristallnacht, or the Night of Broken Glass, is an event that occurred in Nazi Germany on November 9 and 10, 1938. During this

training and experience and familiarity with this investigation, I believe that CC1 meant that synagogues should be spray-painted with anti-Semitic graffiti. CC1 further elaborated on his instructions to other Base members, stating that "if there's a window that wants to be broken, don't be shy." CC1 told the FBI that the operation was nationwide, and that CC1 knew members of The Base's Great Lakes cell carried out attacks against synagogues in Wisconsin and Michigan.

10. CC1 stated that the person who carried out the attack on the synagogue in Racine, Wisconsin, was a Base member known as "Joseph" or "Josef." CC1 stated that Joseph was a member of The Base's Great Lakes cell and was from Wisconsin. CC1 stated that Joseph joined The Base around March 2019, and had been vetted by the group's leader. According to CC1, after the Racine synagogue attack, Joseph sent CC1 a message on an encrypted platform with a news article about the attack and wrote something to the effect of "here's what I did."

11. CC1 stated that CC1 had never met Joseph in person. But, they had communicated with each other via an encrypted message application, which can be

time, Jewish homes, hospitals, and schools throughout Germany were ransacked and demolished by Nazi paramilitary soldiers and civilians. The name "Kristallnacht" comes from the shards of broken glass that littered the streets after the windows of Jewish-owned stores, buildings, and synagogues were smashed.

accessed via computer, cell phone, or other electronic device such as a tablet. CC1 knew Joseph to be a large individual as Joseph's large size was a common joke in The Base chat rooms. CC1 and Joseph had planned to meet in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting.

12. Information provided by CC1 has been corroborated by investigators. For instance, in November 2019, the FBI obtained a search warrant for CC1's residence and electronic devices. In CC1's electronic devices, investigators found evidence showing that that around September 17, 2019, and again on September 21, 2019, CC1 conducted multiple Google searches for "Kristallnacht." Following the search for "Kristallnacht" on September 17, 2019, CC1 used an internet browser to access an encrypted messaging application known to be utilized by members of The Base. The digital evidence showed that CC1 accessed the encrypted messaging application and visited a section of the application that was labeled with the symbol for The Base.

13. On September 23, 2019, CC1 conducted multiple Google searches for "racine, wi," "racine wi nazi," and "racine wi anti-semitic." CC1 also accessed news websites and Twitter that had posted articles and comments on the Racine synagogue vandalism. Further, the device evidence shows that on September 23,

2019, CC1 accessed the same encrypted messaging application noted above. The evidence showed that CC1 accessed a section of the encrypted messaging application that was labeled with "JOSEPH." Based on my training and experience and my involvement in this investigation, I believe that CC1 was using the encrypted messaging application to exchange messages with members of The Base, including Joseph.

14. As part of the FBI's investigation into the Base, an FBI undercover employee (UCE) gained access to The Base's members-only chat room on the encrypted messaging application discussed above. This included a group chat in September 2019 among several individuals in which CC1, utilizing his known Base online moniker, urged other members of the group chat to respond to the doxing² of a Base member. CC1 directed that between September 20-25, 2019, CC1 wanted them to "get out and act. Flyers, windows, and tires." He also told members of the group chat that arsons, breaking windows, and slashing tires are near impossible to track. In response to CC1's call to action, a chat member named Joseph responded

² Based on publicly available information, I am aware that "doxing" is the online practice of researching and broadcasting private or identifying information about an individual or organization. The methods employed to acquire this information include searching publicly available databases and social media websites, hacking, and social engineering. Doxing is often done with malicious intent.

"I agree with that . . . calculated action" and tagged CC1's online moniker. Joseph went on to write "imagine if across the country on local news, Everyone is reporting on new nazi presence." CC1 in the same chat wrote "20th—25th, vandalize my friends. We'll push back on the enemy as they push bacjk [sic]." Another member of the chat wrote "No point in random vandalizing... Much more effective if its targeted," to which Joseph responded "^^ MAKE IT WORTH IT." As part of the chat, CC1 wrote "Kristallnacht" and Joseph wrote "Take your time, plan your out your AO." Later on in the group chat, Joseph wrote "Our op will be a perfect fuck you to these kikes if we become terrorists." CC1 later wrote a long entry titled "Operation Kristallnacht," discussing why this was the time to act, to which Joseph responded "Sieg Heil."

15. CC1 has been arrested and charged in another federal district court with violating 18 U.S.C. § 241. The charges relate to CC1's conduct in directing other Base members to attack synagogues in Racine, Wisconsin, and Hancock, Michigan, as described above.

16. As noted above, during CC1's interviews with the agents, he stated that he had planned to meet Joseph in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting. As discussed below, that Base meeting did occur in Silver Creek, Georgia, from about

October 30, 2019 until November 2, 2019, and that the Base member known as Joseph attended the meeting.

17. Between October 31 and November 3, 2019, the UCE participated in an “in real life” or “IRL” meeting of The Base at the residence of a Base member in Silver Creek, Georgia. About a dozen individuals participated in the event, including the Base member known as Joseph. The meeting included firearms training, grappling, and basic medical training, and a pagan “blot” ritual where a goat was sacrificed. UCE observed Joseph participate in many of these activities.

18. The Base member known as Joseph was observed by the FBI arriving and departing this meeting while driving a dark GMC SUV bearing Wisconsin license plate 671NGF. Records show that the vehicle with this plate is a 2008 GMC Acadia with VIN# 1GKER13748J138676 and registered to an individual with initials O.B. with an address 1101 E Forest Hill Avenue, Oak Creek, Wisconsin 53154 (Subject Residence). Yousef Omar Barasneh, is the adult son of O.B. and resides at the Subject Residence. Records from the State of Wisconsin show that Yousef Omar Barasneh was born 11/26/1997, lists 1101 E Forest Hill Avenue, Oak Creek, Wisconsin, as his residence, and that he is 6’2” and 300 lbs.

19. I have reviewed images of Joseph from the Base meeting in Georgia, and Yousef Omar Baresneh’s Wisconsin Driver’s License photo, and I believe that

The Base member known as Joseph is Yousef Omar Barasneh. Further, on November 15, 2019, November 25, 2019, December 5, 2019, and January 10, 2020, the FBI observed Yousef Omar Barasneh driving the Subject Vehicle in and around Oak Creek, Wisconsin.

20. As part of the investigation, I reviewed information from Wyndham Hotels and Resorts showing that on October 30 to 31, 2019, Yousef Omar Barsneh registered to stay at a La Quinta Inn located at 15 Chateau Dr. SE, Rome, Georgia, and provided a home address of 1101 Forrest Hill Avenue, Oak Creek, WI 53134. That hotel is approximately seven miles from the Base residence in Silver Creek, Georgia, where the Base meeting took place that same weekend.

21. As part of the investigation, FBI agents identified several dates and locations where members of the Base were believed to have been. This included (1) July 27, 2019, the date that The Base conducted training at the Wood County Firing Range, 3705 Marsh Road, Town of Seneca, Wood County, WI 54495; and (2) the evening of September 21, 2019, when the Beth Israeli Sinai Congregation located at 3009 Washington Avenue Racine, Wisconsin, was vandalized.

22. Thereafter, pursuant to a court order, agents obtained information about cell phone connections to towers near those locations on those dates. The cell tower information revealed that, on July 27, 2019, between 7:00 a.m. and 7:00 p.m.,

a device with telephone number 414-418-8150 pinged approximately 78 times off the tower close to 3705 Marsh Road, Town of Seneca, Wood County, WI 54495. The information further showed that on September 21, 2019, between 8:38 p.m. and 9:08 p.m., the device with that number pinged approximately 6 times off the tower close to 3009 Washington Avenue, Racine, Wisconsin.

23. Records obtained from AT&T show that during the relevant time period, the phone number 414-418-8150 has been issued to subscriber O.B. and user Yousef Barasneh, with a billing address 1101 E Forest Hill Avenue, Oak Creek, Wisconsin, 53154. The records from AT&T state that the phone number is associated with an Apple iPhone 6S with IMEI 3557670792347715, though I understand that phone numbers may be ported among devices at any time. Police records further show that on October 24, 2017, Yousef Omar Barasneh had contact with the Oak Creek Police Department and reported to the officers that 414-418-8150 was his (Yousef's) phone number. Records from AT&T further show that, between October 30 and November 2, 2019, the device with phone number 414-418-8150 connected with cell towers near Rome, Georgia, and Silver Creek, Georgia.

24. Based on my training and experience, I know that most individuals keep personal items such as credit cards, identification, and cell phones close to them, often on their person, in their residence, or in their vehicle.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises and Subject Vehicle, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including cell phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause.* I submit that if a computer or storage medium is found, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the subject premises and subject vehicle because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems

can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus

inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline

information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from a premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the

search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

30. Because several people share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

31. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users, and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

32. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password.

These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. Therefore, I request that this warrant permit law enforcement agents to obtain from Yousef Omar Barasneh the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the device(s).

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the frontfacing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable

the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

37. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices are subject to search and seizure pursuant to the applied-for warrant. The passcode or password that would unlock such device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48

hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the

device(s) in order to search the contents as authorized by this warrant.³

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to search the properties described in Attachment A and seize the items described in Attachment B.

³ The proposed warrant does not authorize law enforcement to require that the aforementioned person state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant.

ATTACHMENT A

Property to be searched

The property to be searched is further described as follows:

- The premises known as 1101 E Forest Hill Avenue, Oak Creek, Wisconsin, more particularly described as a two-story white and brown house with an attached garage and two outer buildings.
- The vehicle identified as a 2008 black GMC Acadia bearing VIN# 1GKER13748J138676 and Wisconsin license plate 671NGF.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 241 (conspiracy against rights), those violations involving Yousef Omar Barasneh ("Barasneh") and occurring after March 1, 2019, including:

- a. Records and information relating to a conspiracy to injure, oppress, threaten, and intimidate minority citizens, including Jewish citizens, in the free exercise of their legal rights, including the right to hold and use real and personal property in the same manner as that right is enjoyed by white citizens, as guaranteed by Title 42, United States Code, Section 1982.
- b. Records and information relating the organization known as The Base, associates of The Base, or white supremacy ideology, including any communications;
- c. Records and information relating to the Beth Israeli Sinai Congregation;
- d. Records and information relating to targets or potential targets of threats, harassment, or intimidation by the Base or otherwise based on white supremacist ideology;

e. Clothing and other items worn or used by the suspect during activities associated with The Base or in furtherance of violations of 18 U.S.C. § 241, including any preparatory activities;

f. Records and information relating to the identity or location of the suspect, associates, and co-conspirators;

g. Apple iPhone 6S with IMEI 3557670792347715, and any cellular device assigned phone number 414-418-8150.

2. Computers or storage media used as a means to commit the violations described above, including communicating with co-conspirators.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the property described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Barasneh to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Barasneh and activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Barasneh and activate

the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.